UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF MICHIGAN

SCOTT TEMPLE and THOMAS COWAN, individually and on behalf of all others similarly situated, Plaintiffs, v. FLAGSTAR BANCORP, INC. and FLAGSTAR BANK, FSB, Defendants.	Case No. 2:22-CV-11395-LJM-EAS CLASS ACTION JURY TRIAL DEMANDED

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Scott Temple and Thomas Cowan ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this First Amended Class Action Complaint against Defendants Flagstar Bancorp, Inc. and Flagstar Bank, FSB (collectively, "Flagstar"), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Flagstar for its failure to secure and safeguard their and approximately 1,547,169 other individuals' private and

confidential personally identifiable information ("PII"), including at least their names and Social Security numbers.

2. Between December 3, 2021, and December 4, 2021, unauthorized individuals gained access to Flagstar's network systems and accessed and acquired files from the system that contained the PII of Plaintiffs and Class members (the "Data Breach").

3. Flagstar owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Flagstar breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' and former customers' PII from unauthorized access and disclosure.

4. As a result of Flagstar's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all individuals whose PII was exposed as a result of the Data Breach, which Flagstar first publicly acknowledged on or about June 17, 2022.

5. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence per se, breach of fiduciary duty, breach of express

contract, breach of implied contract, unjust enrichment, violation of the Utah Consumer Sales Practices Act, violation of the California Consumer Protection Act of 2018, and violation of the California Unfair Competition Law, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

6. Plaintiff Scott Temple is a Utah resident. He provided his PII to Flagstar in connection with receiving financial and/or mortgage-related services. Had Plaintiff known that Flagstar does not adequately protect PII, he would not have used Flagstar's services, and would not have agreed to provide Flagstar with, or allow Flagstar to maintain, his PII.

7. Plaintiff Thomas Cowan is a California resident. He provided his PII to Flagstar in connection with receiving mortgage-related services. Had Plaintiff Cowan known that Flagstar does not adequately protect PII, he would not have used Flagstar's services, and would not have agreed to provide Flagstar with, or allow Flagstar to maintain, his PII.

8. Defendant Flagstar Bancorp, Inc. is a corporation that was formed in Michigan and has its principal place of business in Troy, Michigan. Flagstar's corporate headquarters are located at 5151 Corporate Drive, Troy, Michigan 48098.

9. Defendant Flagstar Bank, FSB is a Michigan-based federally chartered stock savings bank with its corporate headquarters located at 5151 Corporate Drive, Troy, Michigan 48098.

JURISDICTION AND VENUE

10. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

11. This Court has personal jurisdiction over Flagstar because Flagstar is a corporation organized under the laws of Michigan and conducts significant business in Michigan.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Flagstar's principal place of business is located in Troy, Michigan.

FACTUAL ALLEGATIONS

Overview of Flagstar

13. Flagstar is a bank headquartered in Troy, Michigan. Flagstar has numerous branch and home loan center locations across the United States and is one of the largest residential mortgage servicers in the country.

14. Flagstar operates 150 branches in Michigan, Indiana, California, Wisconsin, and Ohio, and its mortgage divisions operates nationally with 82 retail locations. With assets of $31 billion, Flagstar touts that it is the sixth largest bank mortgage originator nationally and the second largest savings bank in the country.[1]

15. Flagstar has a page on its website entitled "Privacy" which states, "Flagstar Bank is committed to protecting and safeguarding your personal information."[2] From this webpage, customers can access Flagstar's privacy policy, which is entitled "About Your Privacy."[3] The privacy policy states, "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[4]

16. Flagstar's website also contains a page entitled "Data Security and Customer Privacy."[5] There, Flagstar claims, "We've built processes to identify cybersecurity threats and ensure our data and customer privacy are well-protected,"

[1] FLAGSTAR BANK, *About Flagstar*, https://www.flagstar.com/about-flagstar.html (last visited June 21, 2022).
[2] FLAGSTAR BANK, *Privacy*, https://www.flagstar.com/legal-disclaimers/privacy.html (last visited June 21, 2022).
[3] FLAGSTAR BANK, *About Your Privacy*, https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf (last visited June 21, 2022).
[4] *Id*.
[5] FLAGSTAR BANK, *Data Security and Customer Privacy,* https://www.flagstar.com/esg/governance/data-security-and-customer-privacy.html (last visited June 21, 2022).

and also states, "Flagstar's Chief Information Security Officer (CISO) regularly conducts a comprehensive evaluation and testing of our information security program."[6]

17. Plaintiffs and Class members are, or were, customers of Flagstar or received services from Flagstar and entrusted Flagstar with their PII.

The Data Breach

18. Between December 3, 2021, and December 4, 2021, an unauthorized individual, or unauthorized individuals, gained access to Flagstar's network systems and accessed and acquired certain files on Flagstar's computer systems.

19. Flagstar did not begin to notify government agencies or the public directly about the Data Breach until over six months after the Data Breach, on or about June 17, 2022. As of June 22, 2022, Flagstar has not posted a notice of the data breach on its website.

20. In Flagstar's notification of the breach to the Office of the Maine Attorney General, it notes that the information acquired by the cybercriminals in the Data Breach includes names or other personal identifier in combination with Social Security numbers.[7]

---

[6] *Id.*

[7] https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml

Flagstar Knew That Criminals Target PII

21. At all relevant times, Flagstar knew, or should have known, its customers', former customers', Plaintiffs', and all other Class members' PII was a target for malicious actors. Flagstar should have been particularly aware of this fact because its customers' and former customers' information was involved in a data breach involving Flagstar's third-party file sharing vendor, Accellion, Inc., less than a year prior to the Data Breach.[8] Despite such knowledge, Flagstar failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII from cyber-attacks that Flagstar should have anticipated and guarded against.

22. PII is a valuable property right.[9] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[10] American companies are estimated to have spent over $19 billion on

[8] Charlie Osborne, *Flagstar Bank Customer Data Breached Through Accellion Hack*, ZDNET (Mar. 8, 2021), https://www.zdnet.com/article/flagstar-bank-customer-data-breached-through-accellion-hack/.

[9] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

[10] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

acquiring personal data of consumers in 2018.[11] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

23. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

24. Consumers place a high value on the privacy of that data. Researchers have shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[12]

25. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that

[11] IAB Data Center of Excellence, U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[12] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

26. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[13]

27. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[14] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks;

[13] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited June 21, 2022).

[14] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[15]

28. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[16]

29. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

30. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer

[15] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[16] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited June 22, 2022).

systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[17]

31. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[18]

32. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiffs and the Other Class Members

33. Plaintiffs and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort

[17] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[18] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Flagstar's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

34. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

35. Plaintiffs bring this action on behalf of themselves and all other members of the following Class of similarly situated persons:

> All individuals whose PII was accessed by unauthorized persons in the Data Breach, including all individuals who are sent a notice of the Data Breach.

36. Excluded from the Class is Flagstar Bancorp, Inc. and Flagstar Bank, FSB and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

37. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

38. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Flagstar reported to the Maine Attorney General that approximately 1,547,169 individuals' information was exposed in the Data Breach.

39. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Flagstar had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;

b. Whether Flagstar failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII;

c. Whether an implied contract existed between Class members and Flagstar providing that Flagstar would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

d. Whether Flagstar breached its duties to protect Plaintiffs' and Class members' PII; and

e. Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

40. Flagstar engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

41. Plaintiffss claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Flagstar, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

42. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

43. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate

their claims against Flagstar, so it would be impracticable for Class members to individually seek redress from Flagstar's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

44. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

45. Flagstar owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

46. Flagstar knew the risks of collecting and storing Plaintiffs' and Class members' PII and the importance of maintaining secure systems. Flagstar knew of the many data breaches that targeted companies that stored PII, including itself, in recent years.

47. Given the nature of Flagstar's business, the sensitivity and value of

the PII it maintains, and the resources at its disposal, Flagstar should have identified the vulnerabilities to their systems, let alone never permitting them and correcting them when found, and prevented the Data Breach from occurring.

48. Flagstar breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiffs' and Class members' PII.

49. It was reasonably foreseeable to Flagstar that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

50. But for Flagstar's negligent conduct and breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

51. As a result of Flagstar's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach,

Plaintiffs and Class members have suffered, and will continue to suffer, economic damages, and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Flagstar's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

52. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

53. Flagstar's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Flagstar, of failing to employ reasonable measures to protect and secure PII.

54. Flagstar violated Section 5 of the FTCA by failing to use reasonable

measures to protect Plaintiffs' and Class members' PII and not complying with applicable industry standards. Flagstar's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

55. Flagstar's violation of Section 5 of the FTCA constitutes negligence per se.

56. Flagstar and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

57. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA weas intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class members as a result of the Data Brach.

58. It was reasonably foreseeable to Flagstar that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII to

unauthorized individuals.

59. The injury and harm that Plaintiffs and Class members suffered was the direct and proximate result of Flagstar's violations of Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Flagstar's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

60. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

61. Plaintiffs and Class members gave Flagstar their PII in confidence, believing that Flagstar would protect that information. Plaintiffs and Class members would not have provided Flagstar with this information had they

known it would not be adequately protected. Flagstar's acceptance and storage of Plaintiffs' and Class members' PII created a fiduciary relationship between Flagstar and Plaintiffs and Class members. In light of this relationship, Flagstar must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiffs' and Class Members' PII.

62. Flagstar has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class members' PII, failing to comply with data security guidelines, and otherwise failing to safeguard Plaintiffs' and Class members' PII that it collected.

63. As a direct and proximate result of Flagstar's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Flagstar's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and

repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF EXPRESS CONTRACT

64. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

65. Plaintiffs and Class members and Flagstar entered into written agreements regarding the services that Flagstar was to provide to Plaintiffs and Class members. Plaintiffs and Class members paid Flagstar monies and provided Flagstar with their PII as consideration for these agreements. Flagstar's document entitled "About Your Privacy" and its webpage entitled "Data Security and Customer Privacy" are evidence that data security was a material term of these contracts.

66. Plaintiffs and Class members complied with the express contract when they paid Flagstar and provided their PII to Flagstar.

67. Flagstar breached its obligations under the contracts between itself and Plaintiffs and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII.

68. Flagstar's breach of the express contracts between itself, on the one hand, and Plaintiffs and Class members, on the other hand directly caused the Data Breach.

69. Plaintiffs and all other Class members were damaged by Flagstar's breach of express contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they endure and will continue to endure.

COUNT V
BREACH OF IMPLIED CONTRACT

70. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

71. In connection with receiving services from Flagstar, Plaintiffs and all other Class members entered into implied contracts with Flagstar.

72. Pursuant to these implied contracts, Plaintiffs and Class members provided Flagstar with their PII in order for Flagstar to service their loans, for which Flagstar is compensated. In exchange, Flagstar agreed to, among other things, and Plaintiffs understood that Flagstar would: (1) provide services to

Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3) protect Plaintiffs' and Class members PII in compliance with federal and state laws and regulations and industry standards.

73. The protection of PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Flagstar, on the other hand. Indeed, Flagstar was clear in its statements regarding customer privacy, and Plaintiffs understood, that Flagstar supposedly respects and is committed to protecting customer privacy.

74. Had Plaintiffs and Class members known that Flagstar would not adequately protect its customers' and former customers' PII, they would not have provided Flagstar with their PII.

75. Plaintiffs and Class members performed their obligations under the implied contracts when they provided Flagstar with their PII.

76. Flagstar breached its obligations under their implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

77. Flagstar's breach of its obligations of its implied contracts with

Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

78. Plaintiffs and all other Class members were damaged by Flagstar's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they endure and will continue to endure.

COUNT VI
UNJUST ENRICHMENT

79. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

80. This claim is pleaded in the alternative to the breach of express and implied contract claims.

81. Plaintiffs and Class members conferred a monetary benefit upon Flagstar in the form of monies paid for services which were not provided in full.

82. Flagstar accepted and had knowledge of the benefits conferred upon it by Plaintiffs and Class members. Flagstar benefitted from the receipt of Plaintiffs' and Class members' PII, as this was used to facilitate payment.

83. As a result of Flagstar's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

84. Flagstar should not be permitted to retain the money belonging to Plaintiffs and Class members because Flagstar failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

85. Flagstar should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of its conduct relating to the Data Breach alleged herein.

COUNT VII
VIOLATION OF THE UTAH CONSUMER SALES PRACTICES ACT
Utah Code §§ 13-11-1, *et seq.* ("UCSPA")

86. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

87. Plaintiffs and Flagstar are "persons," as defined by Utah Code § 13-11-1(5).

88. Flagstar is a "supplier," as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces "consumer transactions," as defined by Utah Code § 13-11-1(2).

89. Flagstar engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of UCSPA, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect the PII of Plaintiffs and Class members, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the data breach;

c. Failing to comply with, and omitting, concealing, and suppressing noncompliance with, common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Utah Protection of Personal Information Act, Utah Code § 13-44-201, which was a direct

and proximate cause of the data breach; and

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class members' PII.

90. Flagstar intended to mislead Plaintiffs and Class members and induce them to rely on its omissions.

91. Flagstar's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Flagstar's data security and ability to protect the confidentiality of PII.

92. Had Flagstar disclosed to Plaintiffs and Class members that its customers' PII was vulnerable to attack, it would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

93. Flagstar had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the PII in its possession. Flagstar's duty to disclose arose from its possession of exclusive knowledge regarding the security of the data in its systems and its active concealment of the state of its security.

94. Flagstar intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by: indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics,

accessories, uses, or benefits, if it has not; indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not; indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not.

95. Flagstar engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, and unjustly imposed hardship on Plaintiffs and the Class by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity; and lost value of their PII. The deficiencies in Flagstar's data security, and the material omissions concerning those deficiencies, led to unfair surprise to Plaintiffs and the Class when the Data Breach occurred.

96. As a direct and proximate result of Flagstar's unconscionable and deceptive acts or practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

97. Flagstar's violations present a continuing risk to Plaintiffs and Class members as well as to the general public.

98. Plaintiffs and Class members in Utah seek all monetary and non-monetary relief allowed by law, including actual damages pursuant to Utah Code §§ 13-11-19, *et seq.*; injunctive relief; and reasonable attorneys' fees and costs.

99. In accordance with Utah Code § 13-11-21(2), counsel for Plaintiffs will mail by certified mail with return receipt requested a copy of this Complaint to the Utah Division of Consumer Protection.

COUNT VIII
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018

Cal. Civ. Code §§ 1798.100, *et seq*. ("CCPA")

100. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

101. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

102. Plaintiffs and Class members are "consumers" as defined by California Civil Code section 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

103. Flagstar is a "business" as defined by California Civil Code section 1798.140(c) because Flagstar:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its

annual revenues from selling consumers' personal information.

104. Plaintiffs' and Class members' PII was subject to unauthorized access and exfiltration, theft or disclosure because of Flagstar's inadequate security measures.

105. Plaintiffs' and class members' PII was in nonencrypted and nonredacted form, allowing criminals full access to it.

106. The Data Breach occurred as a result of Flagstar's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

107. Attached as Exhibit A is written notice Plaintiffs provided to Flagstar pursuant to California Civil Code section 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Flagstar has or is violating. Although a cure is not possible under the circumstances, if as expected Flagstar is unable to cure or does not cure the violation within 30 days, Plaintiffs will amend this complaint to pursue actual or statutory damages as permitted by California Civil Code section 1798.150(a)(1)(A).

108. As a result of Flagstar's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs seek actual damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT IX
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
(the "UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq*.

109. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

110. The California Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq.*, prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Flagstar engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

111. In the course of conducting its business, Flagstar committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, the FTCA, UCSPA, and CCPA. Plaintiffs and Class members reserve the right to allege other violations of law by Flagstar constituting other unlawful business acts or practices. Flagstar's above-described wrongful actions,

inaction, omissions, and want of ordinary care are ongoing and continue to this date.

112. Flagstar's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Flagstar's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Flagstar's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, UCSPA, and the FTCA. The gravity of Flagstar's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Flagstar's legitimate business interests other than engaging in the above-described wrongful conduct.

113. The UCL also prohibits any "fraudulent business act or practice." Flagstar's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

114. The injury and harm that Plaintiffs and Class members suffered were the direct and proximate result of Flagstar's violations of the UCL. Plaintiffs and Class members have suffered (and will continue to suffer)

economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Flagstar's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

115. Unless restrained and enjoined, Flagstar will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class members, and the general public, also seek restitution and an injunction prohibiting Flagstar from continuing such wrongful conduct, and requiring Flagstar to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. and Prof. Code § 17203.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their and the Class's favor and against Flagstar as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives and appointing Plaintiffs' designated counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Flagstar from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide and extend credit monitoring services and insurance and similar services to protect against all types of identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, and service award, as allowable; and

F. Awarding Plaintiffs and the Class such other relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this First Amended Class Action Complaint so triable.

Dated: June 27, 2022

Respectfully submitted,

/s/ Caleb Marker
CALEB MARKER (MI Bar # P70963)
Caleb.Marker@zimmreed.com
ZIMMERMAN REED LLP
6420 Wilshire Blvd. Suite 1080
Los Angeles, CA 90048
Tel: 877.500.8780
Fax: 877.500.8781

JASON P. JOHNSTON*
jason.johnston@zimmreed.com
RACHEL K. TACK*
rachel.tack@zimmreed.com
ZIMMERMAN REED LLP
1100 IDS Center
80 S 8th Street
Minneapolis, MN 55402
Tel: 612.341.0400
Fax: 612.341.0844

BEN BARNOW*
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL*
aparkhill@barnowlaw.com
RILEY W. PRINCE*
rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.

205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504

*admission pursuant to LR 83.20 to be sought